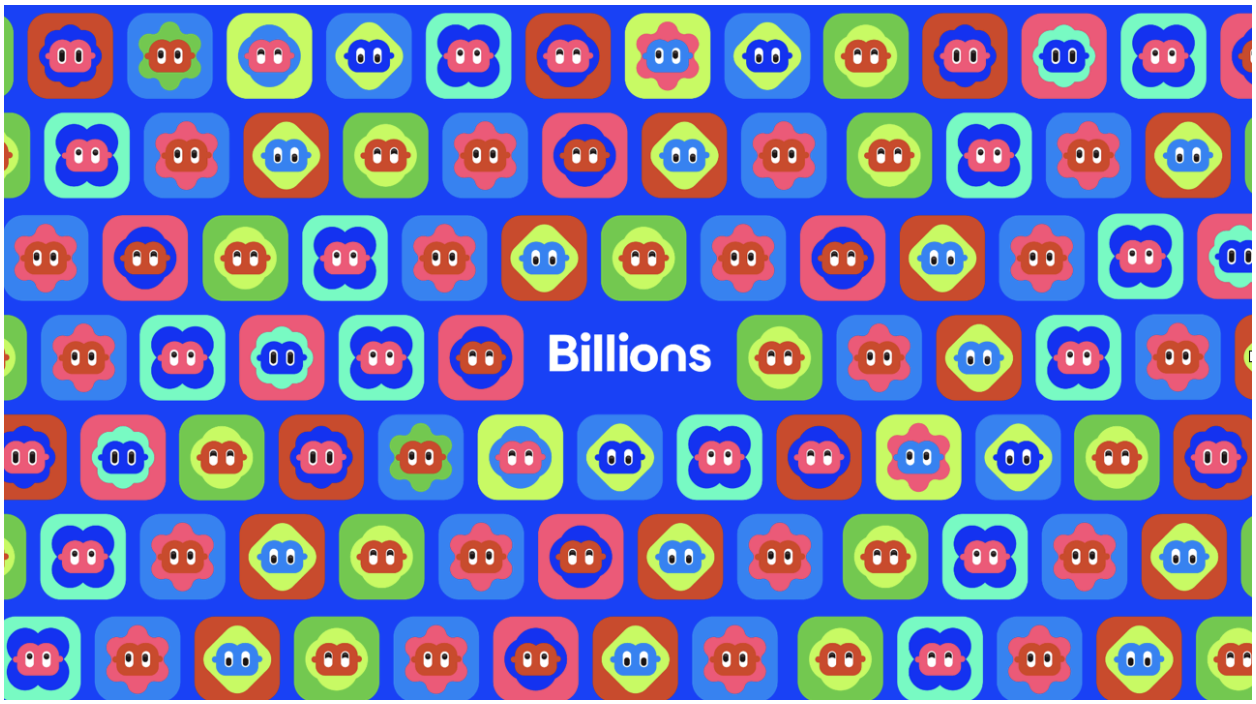
# Billions Network

# White Paper

## The Human and AI Network



## Executive Summary

*Secure, portable trust for the Agentic future at scale*

*$BILL enables verification across the network*

Billions is building the trust layer for the new internet: a world where humans and AI agents coexist, collaborate, and transact with verified integrity. Using decentralized identifiers (DID), verifiable credentials (VC), and verifiable proofs, Billions enables secure, portable verification so anyone, or anything, can prove what's true without revealing more than necessary. Proofs anchor on a rollup secured by Ethereum while preserving unlinkability across applications.

**Problem**. Digital authenticity is failing: bots and multi-wallet farms distort incentives; compliance is siloed and costly; AI agents act without verifiable provenance or policy constraints.

**Solution**. A standards-aligned stack (mobile/web wallets, Issuer Node, Verifier SDK, and a universal onchain verifier) makes verification feel like login. One onboarding; many proofs; selective disclosure by default. $BILL is an ERC-20 on Ethereum (L1); proofs, attestations, and reputation run on Billions L2 with finality on Ethereum.

**What it enables.** Sybil-resistant distribution, reusable KYC/AML, age verification, and Know-Your-Agent (KYA) for accountable AI. Revocation and recovery preserve security; pairwise DIDs prevent cross-app correlation.

**Token utility**. $BILL powers verification payments, staking-based reputation, and ecosystem incentives. It is a utility token; it does not grant ownership, dividends, or corporate voting rights.

**MiCA capsule**. Classification: "other crypto-assets" (utility). Not an e-money token (EMT) or asset-referenced token (ART). Governance is limited to product parameters; treasury operations are rule-based and revenue-funded.

**Road ahead**. Early integrations prioritize Web3 distribution, fintech onboarding, and agent provenance; the roadmap expands to enterprise identity and policy-proofed agents.

# Introduction - Trust for Humans and AI

*Trust makes the internet usable*

*Verification must be security-first*

Billions introduces a verifiable trust layer using decentralized identifiers (DIDs), verifiable credentials (VCs), and verifiable proofs. The system is designed to minimize data exposure while enabling strong assurances of personhood and agent accountability.

The network operates on a rollup anchored to Ethereum for scalability and security, with identity state anchoring and security-preserving revocation mechanisms.

Billions Network is the human-and-AI verification layer for the open internet. It delivers security-preserving identity and trust primitives, verifiable proofs, Decentralized Identifiers (DIDs), and Verifiable Credentials (VCs) so applications, enterprises, and autonomous agents can verify *who* or *what* they are without exposing raw data. This enables compliant KYC/AML, proof-of-personhood, Sybil/bot resistance, and accountable AI interactions across Web3 and enterprise systems.

The network is grounded in our DeepTrust framework: a multidimensional model of agent identity architectural, behavioral, legal, and social anchored by verifiable identifiers and reputation-bearing attestations. By combining DID-based authentication with selective disclosure via verifiable proofs, Billions lets humans and AI prove attributes and relationships while preserving security.

Billions ships a full, standards-aligned stack: web and mobile identity wallets for users; an Issuer Node for credential providers; a Verifier SDK and Universal OnChain Verifier for apps; a set of tailored resources and the most popular OpenClaw identity skills well-suited to agent developer needs; the and a public attestation/registry layer for cross-app trust. These components are already used across Web3 and enterprise contexts to streamline secure onboarding, authorization, and compliance.

Under the hood, Billions operates a Polygon CDK–based Layer-2 optimized to anchor DID state updates and credential attestations, while remaining chain-agnostic through SDKs and multi-network deployments. This design delivers low-latency verification, auditability, and portability of trust across ecosystems.

Economic alignment is provided by the network's native token, used to pay verification fees, bond/stake attesters and verifiers, and enable progressive governance as decentralization increases tying value directly to network usage and the growth of the identity and reputation graph.

Together, these building blocks make Billions a scalable, security-first trust fabric for people, organizations, and AI agents.

## The Problem: A Crisis of Trust and Access

The internet is at a critical inflection point. The rapid integration of AI is eroding digital trust, while systemic identity failures leave billions vulnerable.

- **The Crisis of Authenticity:** Fraud, scams, deep fakes, and malicious bots are rampant, responsible for over $30 billion in losses annually. In Web3, this manifests as Sybil attacks, where bots and multi-wallet farmers dilute reward pools, making fair value distribution ineffective. In Web2 customers are constantly bombarded with questionable emails, text messages, and phone calls that claim to be from a reputable company, but cannot be easily verified.
- **The Crisis of Access:** Over 4 billion people lack stable, digital IDs, excluding them from the global digital economy, finance, and civic life.

The trust gap online is widening in Web3 and across the broader internet due to three reinforcing issues:

- **Sybil/bot proliferation & fragmented KYC.** Airdrops, DAOs, and consumer apps leak value to duplicate or inauthentic accounts; enterprises face high-friction onboarding, inconsistent risk controls, and security liability. Billions targets this with reusable, security-preserving credentials instead of raw-data hand-offs.
- **AI agents without verifiable identity.** Autonomous agents increasingly act, transact, and attest but lack portable, cryptographically verifiable identifiers, which prevents accountability and reputation from forming. A trust system must begin with identity (unique, provable, non-spoofable).
- **Multi-chain and cross-system silos.** Credentials, proofs, and attestations are often trapped per-chain or per-vendor, limiting reuse and composability; verification needs to work off-chain (web/app) and on-chain (smart contracts), across networks.

What the humanity needs now:

- **Portable, security-first verification** that works for humans and AI, supports selective disclosure, and minimizes PII exposure.
- **Universal, chain-agnostic attestations** verifiable off-chain and on-chain, with clear routing for dApps and enterprise systems.
- **Commercial alignment**: fees tied to verification usage, simple SDKs for rapid integration, and incentives that reward quality attesters and compliant apps.

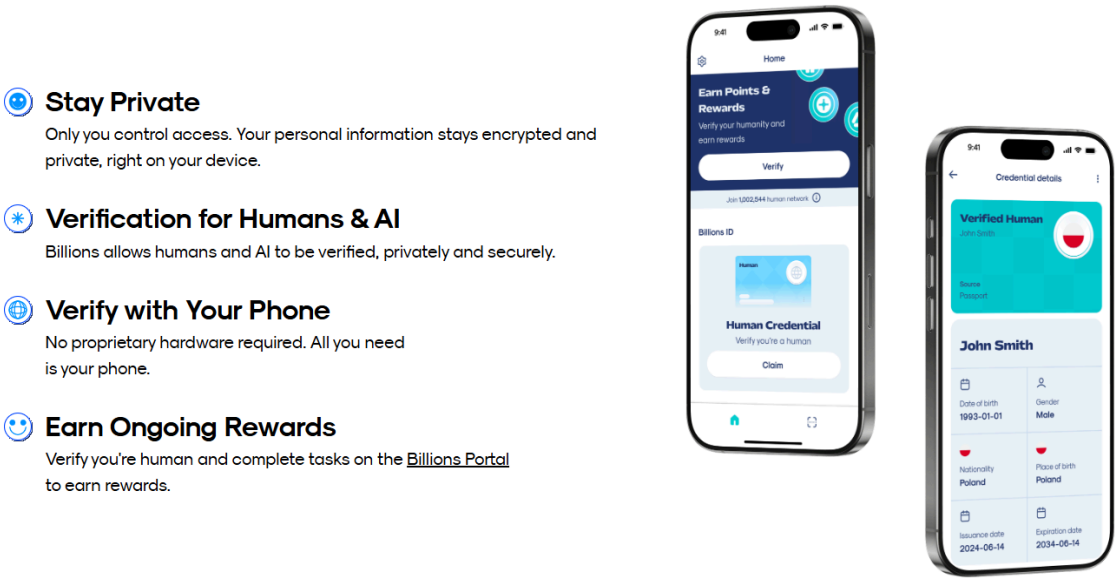
## The Vision: Trust for Humans and AI

Billions' mission is to **save the internet in the age of AI**. Our vision is a connected world where everyone, human or AI, can prove who they are in a secure, verifiable way from their own device. We introduce a verifiable trust layer using DIDs, VCs, and verifiable proofs.

Live web and mobile wallets, issuer/verifier tooling, and a registry architecture meet current Web3 demand and enterprise risk standards, with documented traction and deployment scope.

The system is designed to be:

- **Accessible: Verify with your phone no proprietary hardware**. We use everyday consumer devices and government IDs.
- **Secure:** Users prove attributes without compromising their underlying data.
- **Scalable:** The network operates on a rollup anchored to Ethereum for scalability and security.




## Solution & Architecture

*Onboard once. Prove everywhere.*

*Verify with your phone no proprietary hardware.*

The process is designed for simplicity and security: Onboard once. Prove everywhere.

- **Mobile-First Onboarding:** Users onboard using the Billions mobile app or an embedded web wallet.
- **Progressive Verification:** Users receive credentials from issuers and store them in their self-sovereign wallet. This can include:
    - **Social Verification:** Linking and verifying social profiles.
    - **Liveness:** An on-device scan to prove the user is a live person.
    - **Uniqueness:** An NFC passport scan or national ID validation.
    - **KYC/AML:** Checks against sanction lists and Politically Exposed Persons (PEPs)
- **security-Preserving Proof:** Verifiers request proof (e.g., "Are you over 18?"). The user responds with a verifiable attestation that confirms the fact without exposing the raw data (like their birthdate).
- **Developer Integration:** Integrators use the **Issuer Node** and **Verifier SDK** to issue and verify credentials programmatically in an OAuth-like flow.

- **onchain Finality:** Identity state is batched on the Billions L2 with verifiable proofs and finalized on the Ethereum mainnet
- **Public Profiles:** Enabling Humans, AI Agents, and organizations to build their digital reputation and increase trust in digital interactions.

## Security & security

**Purpose.** Establish clear security guarantees and a threat model for verifiable identity, ensuring unlinkability across verifiers, minimal data exposure, and safe revocation/recovery.

**Design goals.**

- security by default: prove facts (e.g., “over 18?”, “unique human?”, “agent under policy X”) without disclosing raw documents or attributes.
- Unlinkability: pairwise DIDs and selective disclosure prevent correlation across sessions and verifiers.
- Minimized data surface: proofs are generated on-device; only the minimum necessary cryptographic evidence is shared.
- Revocation without exposure: credential revocations are public, but underlying PII never leaves the device.

**Threat model & mitigations.**

- Sybil/bot creation. Mitigated via uniqueness checks (e.g., NFC e-passport/KYC options), attester quality scoring, rate-limits, and staking-based reputation thresholds.
- Cross-verifier correlation. Pairwise DIDs, scoped credentials, nonces bound to verifier domains, and selective disclosure.
- Replay/coercion of proofs. Session-bound challenges, expiry windows, and verifier domain binding.
- Issuer/attester key compromise. Multi-issuer quoruming, key rotation, and revocation registries with onchain audit trails (no PII).
- L2/DA risks. Ethereum L1 finality, data-availability monitoring, circuit testing and audits before upgrades.

**Revocation & recovery.**

- Trigger: device loss, suspected compromise, or issuer policy.
- Effect: proofs derived from revoked credentials fail verification immediately; users re-bind wallet/devices and request re-issuance.
- security: status is checkable without exposing who the subject is or what attributes were proven.

**Unlinkability guarantees (what we commit to).**

- Verifier-to-verifier: the same user appears under different pairwise DIDs.

- Session-to-session: fresh nonces and scoped credentials prevent correlation.
- Attribute-to-identity: verifiers learn only the fact proven, not the underlying attribute or identifier.

**Audits & updates.**

- External security and cryptography audits precede major releases; deprecations and circuit upgrades follow a published schedule with grace periods for integrators.

## Verifications for Humans & AI Agents

*KYC for Humans,  KYA for AI agents*

Establish a multidimensional identity and reputation model -architectural, behavioral, legal, and social- so both humans and agents can be recognized, assessed, and held accountable without exposing raw data. The Billions DeepTrust framework provides features for AI Agents.

**Identifiers & authentication**

- DIDs for agents and humans: with DID-auth flows for human→agent and agent→agent verification (self-verifiable, third-party independent).

**Credentialing & attestations (Hybrid model)**

- Identity Wallets: Hold sensitive Verifiable Credentials as well as credentials  related to the Agent's owner (KYC, age, uniqueness) with selective disclosure and verifiable presentations.
- Public Attestation Registry: Minimal, universal proofs on-chain for permissionless verification and routing. Humans can add proofs via secure queries to protect PII; agents can receive public attestations directly.

**Universal on-chain registry features**

- Cross-chain verifications: Designs for oracle-assisted proof transport so dApps and smart contracts on other networks can consume attestations.
- Verifiable attestations & unlinkability: Pairwise DIDs, selective disclosure, and Data Query Language to prevent correlation while proving facts.

**Reputation composability**

- Graph-based scoring: Combine issuer quality, usage history, dispute rates, endorsements, and quantitative performance into portable trust signals for apps and protocols.

**DeepTrust Framework - Identity for AI Agents**

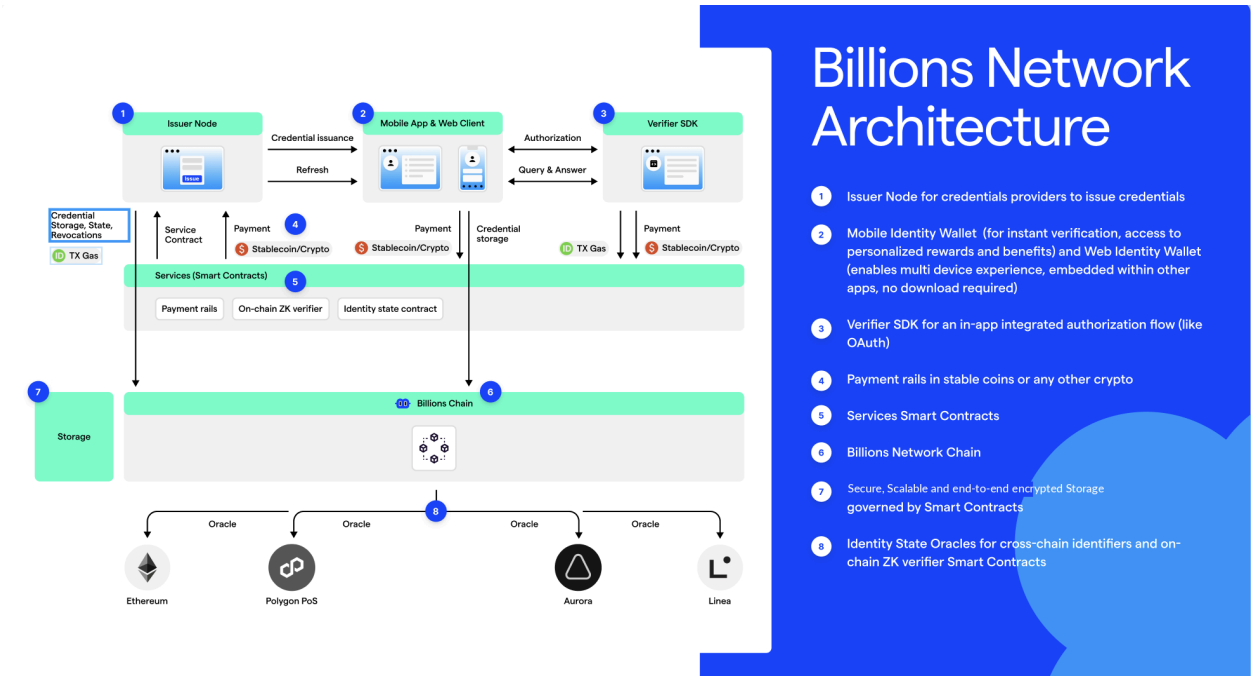
Enables AI Agent Developers to provide verifiable, security-preserving identity and accountability for AI agents without exposing sensitive internals. AI Agents are linked to decentralized identifiers and an Agent Naming System. Agents first obtain a "foundational attestation": which establishes the human/organization that originated the agent identity (first DID-auth evidence), enabling transfer, revocation, or shared ownership via onchain registry.

AI Agents are identified across various dimensions in the framework:

- Architectural identity: Model, weights, code and build provenance, execution environment; anchored by a DID an agent controls (key-based).
- Behavioral identity: Input/output behavior and reproducibility; future-friendly to machine learning when feasible.
- Legal identity: Ownership, certificates, compliance relationships tying agents to accountable entities.
- Social identity: External attestations, endorsements, audits, and performance signals.
- Policy constraints: allowed domains/contracts, spend/action limits, explicit guardrails.
- Operational telemetry: rate limits and audit hooks.

In the DeepTrust verification flow verifiers request policy compliance proofs (e.g., “agent cannot trade above X”); the agent responds with a verifiable proof bound to the verifier domain and session. Sensitive assets (weights, prompts, datasets) remain secure; only compliance facts are proven.

**How Billions implements Human and AI Agent Features**: Delivered through Wallets + Issuer Node + Verifier SDK + Universal On-Chain Verifier atop a Polygon CDK L2 anchor standards-aligned, chain-agnostic, and production-ready for both Web3 and enterprises.




## Key Use Cases

*Airdrops, KYC, age, KYA,Safer DeFi, gaming, exchanges*

The framework is designed to solve critical verification needs for developers and enterprises:

- **Secure Token Distribution:** The most demanded use case in Web3. Billions ensures airdrops, faucets, and rewards go to real, unique human users, preventing Sybil attacks and providing projects with a better ROI on value distribution.

- **Reusable KYC/AML:** A security-preserving solution to verify user identity for compliance. This is critical for RWA (Real-World Asset) tokenization, allowing investors to provide reusable KYC.
- **Age Verification:** A seamless, private way to verify user age for global compliance standards.
- **Know your AI agent (KYA):** Enables agents to securely prove identity, ownership, and reputation providing trust layer across industries like autonomous commerce, AI marketplaces and others.
- **Agent Policy Proofs:** Prove that an AI agent operates under declared constraints (e.g., spend limits, allowed contracts) via policy proofs, without revealing model weights or prompts.
- **Enabling Trust in Digital Business Interactions:** Providing assurance that customers are interacting with genuine representatives of businesses in chat and online meetings.

## Billions (BILL) Tokenomics Overview

*Building the Trust Economy for Humans and AI*

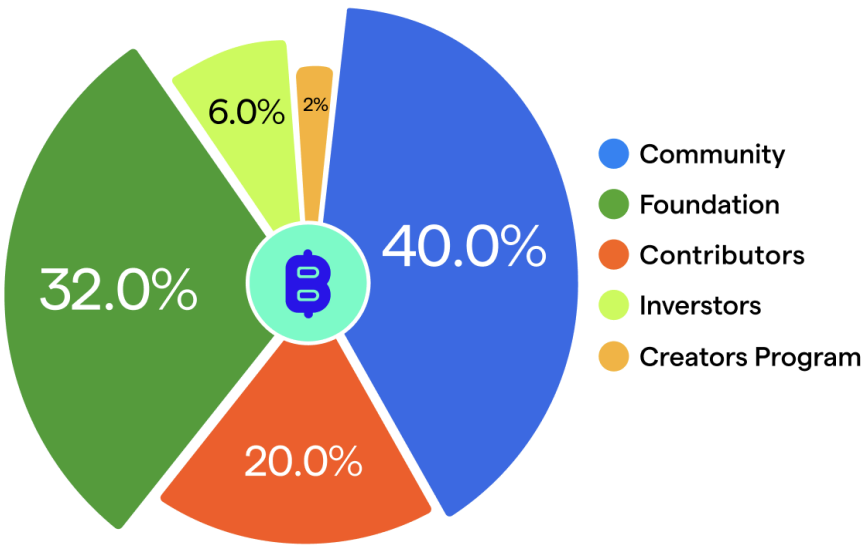
### Summary

Billions Layer-2 establishes the foundation for verifiable identity and trust in decentralized ecosystems. Our tokenomics model aligns economic incentives with long-term network health, prioritizing sustainable value creation over short-term extraction.

### Token Fundamentals

The BILL token maintains a total fixed supply of 10,000,000,000 tokens with zero inflation rate. Built as an ERC-20 token on Ethereum Layer-2, the initial circulating supply at the Token Generation Event (TGE) is around 24.28%, representing around 2.4 billion tokens. The initial circulating supply is designed to support broad network participation from launch.

### Token Allocation



The distribution reflects a community-first approach with the largest allocation directed toward ecosystem participants. The Community receives 40% of total supply, with around 6.28% unlocked at TGE and the remainder distributed over 4 years through front-loaded emissions during the critical bootstrap phase. Contributors, representing the core team and builders, hold 20% with a strict 1-year cliff followed by 3-year linear vesting from Year 2 through Year 4.

Foundation accounts for 32% of supply, split between 16% unlocked at TGE for operational needs and liquidity provision, and 16% locked until Year 2 with linear release of equally distributed allocations through Year 4. This structure ensures the foundation has resources to operate while preventing premature treasury depletion.

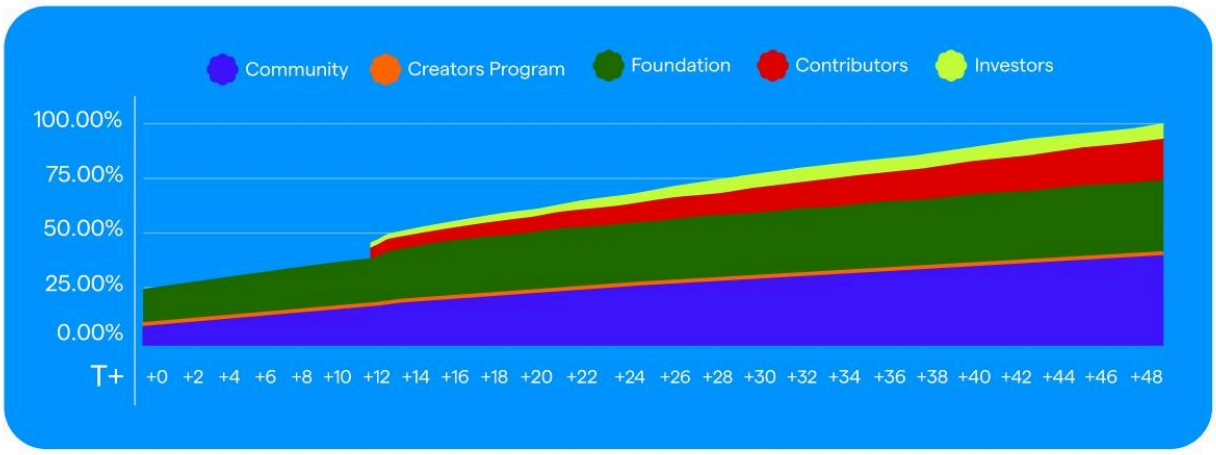
Investors receive 6% with vesting terms over 4 years with 12 month cliffs, with unlocks depending on investment round. The Creators Program allocation holds 2% of the total supply.

**Community Allocation Breakdown**

Within the 40% community allocation, 10% of it flows to staking rewards and incentives to long-term commitment, while remaining funds are used for hackathons and network participant incentives to bootstrap ecosystem activity.

The distribution philosophy emphasizes front-loaded emissions during the first two years when network effects are most critical, then transitions to gradual release through Year 4 as the protocol matures and organic demand sustains growth.

## Supply Release Schedule



At TGE, 24.28% of tokens enter circulation primarily through community allocations, ecosystem fund deployment, and foundation operational reserves. By the end of Year 1, circulating supply reaches around 32% with the first investor and contributors unlocks beginning in year 2. This gradual increase continues as Year 2 ends with around 60% circulating.

Year 3 concludes with 80% of supply in circulation, and finally, by Year 4 end, full token distribution reaches 100% completion. This measured unlock schedule prevents supply shocks while maintaining healthy market liquidity, protecting early investors and community members from excessive dilution.

## Economic Model: Usage-Driven

The revenue model centers on three primary streams.

User verification fees range from $0.50 for basic humanity proofs to $3-5 for full KYC verification, with custom pricing for premium enterprise services. Credential reuse fees create ongoing revenue through small lookup charges, generating near-zero marginal cost income that scales exponentially with network effects.

Premium services including AI agents identity attestations, priority API access, and cross-chain reputation services provide additional high-margin revenue.

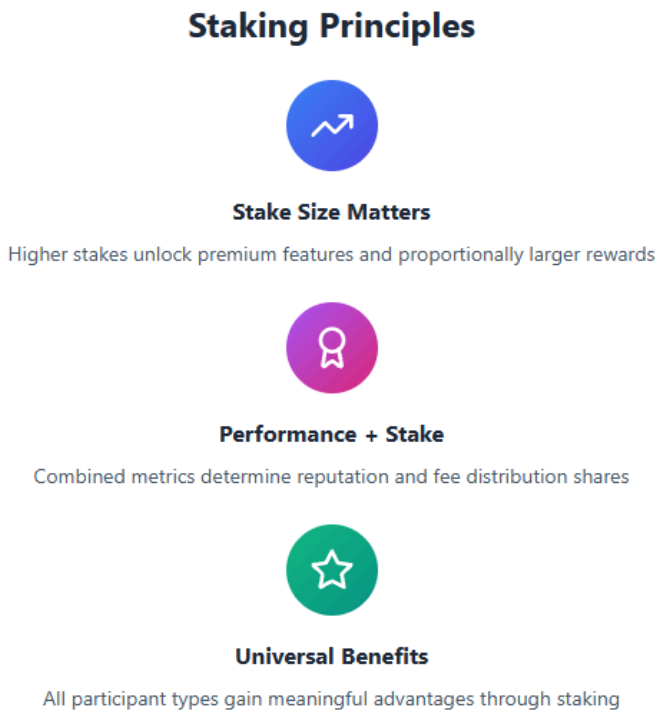
## Token Utility

The BILL token serves multiple critical functions within the Billions ecosystem. Governance rights, to be introduced in future phases, enable token holders to vote on protocol parameters and Trust Registry curator elections.

## Staking for Network Participation

Attesters, the entities issuing verifiable credentials, face strong incentives to stake BILL. The protocol requires or strongly encourages attester staking to participate in the network, with stake size directly influencing reputation coefficients applied to their attestations.

Higher stakes unlock access to premium credential types and premium features based on combined stake and performance metrics.




Individual users stake to enhance their reputation and boost trust scores across the ecosystem. Staked users receive priority access to newly launched credential types and maintain eligibility for promotional campaigns.

Vendors and applications integrating Billions identity services gain substantial advantages through staking. They access higher API rate limits for integration flexibility, receive priority technical support and early feature access, and secure priority queue positions during network capacity constraints.

AI agents represent a novel stakeholder category. Autonomous agents stake BILL as collateral for network operation, signaling trustworthy behavior to potential interaction partners. Stakes grant required permissions for accessing higher-tier data and services, with future protocol versions potentially implementing slashing mechanisms for agent misbehavior as dispute resolution systems mature.

## Value Capture Mechanisms

The network GDP effect creates a dynamic where more users generate more verifications, producing more protocol fees. The critical differentiator lies in reusable credentials creating perpetual revenue streams with zero marginal cost, unlike traditional one-time verification models that must constantly acquire new customers.

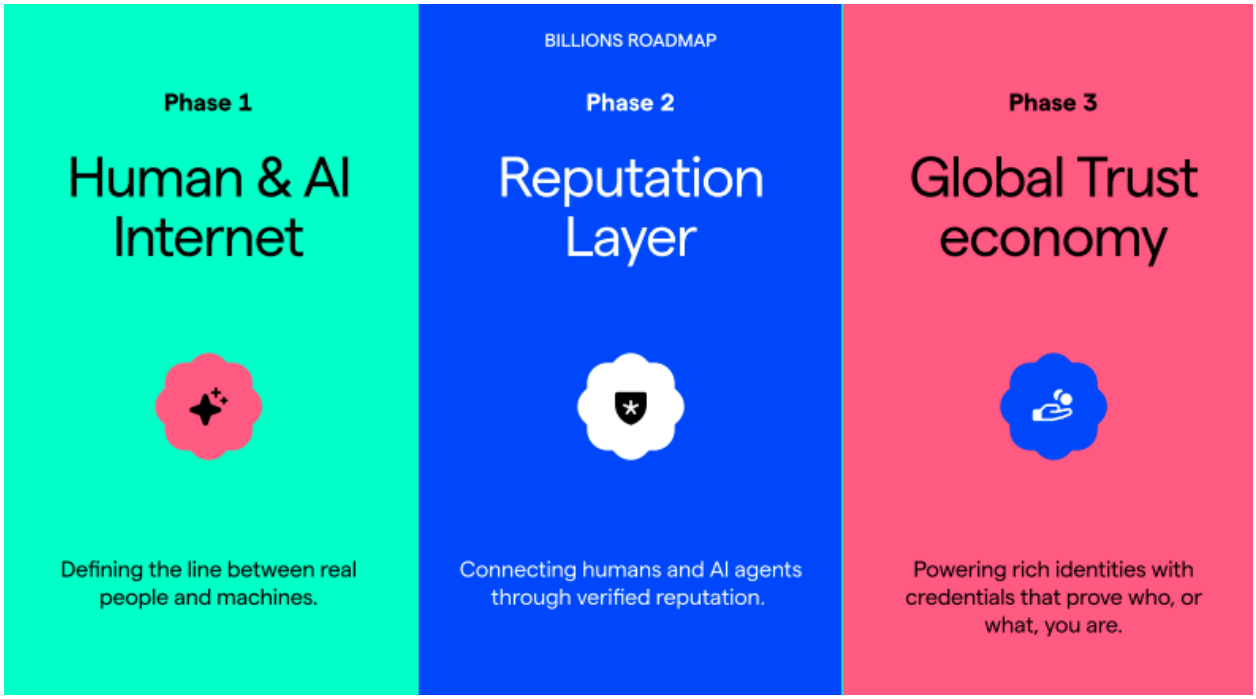
Staking demand emerges organically from multi-stakeholder participation across users, attesters, vendors, and agents. Compound benefits accumulate over time as reputation systems benefit sustained participation.

### Stakeholder Alignment

Early community members receive VIP treatment including priority access to new features, elite verified user pools, and early releases of novel credential types. Portable reputation allows trust credentials to travel seamlessly across the entire ecosystem, and earning opportunities emerge through community agent programs, tutorial creation, and referral systems.

Protocol partners receive integration support and co-marketing resources upon successful deployment. The shared user network allows partners to access Billions' verified user base without requiring redundant KYC processes. Partner status tiers at Basic, Verified and Premium levels provide escalating benefits, while cross-promotion systems incentivize user referrals between applications. Co-marketing initiatives provide joint campaign support from the protocol team.

## Roadmap




The project's execution is structured in four distinct phases:

- **Phase 1 (2025): Preparation and Foundation**
    - Development of the verification features for humans and AI agents.

    - Legal and operational preparations and initial contract audits.
- **Phase 2 (2026): Token Launch and Network Activation**
    - Token Generation Event (TGE) and initial distribution.
    - Initial listings on CEX/DEX and agreements with market makers.
    - Launch of first benefits and user rewards for using credentials.
- **Phase 3 (2026): Expansion of Use Cases & Ecosystem**
    - Growth of the ecosystem with strategic partners in DeFi, gaming, and fintech.
    - Launch of reusable credentials with monetization (recurring revenue from verifications).
- **Phase 4 (2027 onwards): Decentralization and Governance**
    - Introduction of progressive governance mechanisms for non-financial decisionmaking.
    - Expansion of cross-chain compatibility for verifiable identity.

## Standards & Interoperability

**Standards implemented.**

- W3C DID & Verifiable Credentials.
- EVM / ERC-20 / EIP-712 for typed messages and signatures.
- WalletConnect & OAuth-like flows for developer familiarity.
- Polygon CDK rollup architecture; chain-agnostic SDKs.

**Interoperability commitments.**

- Universal onchain Verifier deployed on multiple networks to validate proofs and attestations.
- SDK compatibility with common Web3 wallets and enterprise identity stacks.
- Versioned circuits & schemas with semantic versioning to avoid breaking changes and enable graceful deprecation.

## Adoption & Integrations

Live components. Mobile/web wallet, Issuer Node, Verifier SDK, Agent SDK, and Universal onchain Verifier.

Early integrations.

- Sybil-resistant distribution (airdrops/faucets with uniqueness and bot-resistance).
- Reusable KYC/AML for exchanges/fintech and RWA tokenization.

- Age-gated access (prove “18+” without exposing birth date).
- Agent provenance & policy proofs for accountable AI.

KPIs tracked. Verification volume, credential reuse rate, unique active verifiers, attester quality score, SDK adoption, and revocation/resolution times.

## GDPR / DPIA Summary

**Data minimization**. No biometrics are retained. Proofs are generated on-device; verifiers receive only the minimum cryptographic evidence needed.

**Lawful bases**. Contract/performance for service usage; legitimate interest for fraud/security; explicit consent where required by jurisdiction or use case.

**Rights & controls**. Users can revoke credentials, rotate keys/devices, and request erasure where applicable. Revocation is security-preserving and does not reveal identity or attributes.

**Controller/Processor Roles.** Billions generally acts as a data processor for enterprise customers and integrators, processing personal data only on the documented instructions of the controller. In limited cases (e.g., our public website, product analytics, or direct end-user support), Billions may act as an independent controller. Role allocation and responsibilities are set out in our Data Processing Agreement (DPA).

**Retention.** We retain personal data only for as long as necessary to deliver the service or to comply with legal obligations. Credential status and revocation proofs are public and security-preserving; they do not reveal identity or attributes.

## Appendix

This version is for public communication and may simplify or summarize certain technical, legal, or token-economic aspects.

This summary does not replace the official MiCA-notified document. Classification and compliance information are indicative only.